CLAIMS

I/We claim:

1. A method of organization non-trusting parties with no central administration so that parties can securely share resources and communicate with an expected quality of service.

2. A system of organizing multiple nodes on a network in a hierarchical relationship structure to efficiently inter communicate in a way that optimizes throughput by utilizing hierarchical pathing and an internode hierarchical relationship to provide a shortest route between two nodes, wherein the network has the same structure on every level of the hierarchy.

3. A system that controls resource allocation through inheritance aggregation and hierarchical rights enforcement while allowing for dynamic sub-division and delegation of resource control.

4. A method of network communication that controls node interaction through the exchange of signed documents.

5. A decentralized system for maintaining resource guarantees (quality of service, QOS) dynamically through path rerouting and recombination.

6. A broadcast communication system that allows a single source broadcast to be independently rebroadcast in multiple different time frame groupings.

7. A highly scaleable authentication method that requires the client making a request to a host to securely process portions of authentication request itself.

8. A method of distributing public and private keys in a way which gives each sovereign entity control over key redistribution and allows inter key cooperation when required.

9. A process of utilizing a set of cryptographic primitives (algorithms) to secure and control dynamic routing at the protocol level.

10. A process of choosing communication routes dynamically based on a hierarchical relationship of the nodes comprising a network.

11. A method of establishing a link between nodes that reduces DOS by requiring the node requesting the establishment to perform a computation that is more complex than the computation needed to perform the key exchange.

12. A method of establishing a communications link between two nodes through a cryptographic authentication process, such that the identities of the two nodes are not externally visible over the link.

13. A decentralized method of identity inheritance that is self-authenticating.

14. A decentralized method of quantifying aggregate resource availability for node paths in a network that optimizes routing and distributes communication load.

15. A process to allow permission based network policy control via cryptographically signed documents, which are automatically distributed to the relevant nodes within the network.

16. A method of assigning ownership and priority to network resources that allows resources to be sub divided for use and delegation.

17. A method of cryptographically verifying aggregated inheritance of permissions and enforcing resource allocation by aggregated inheritance priority.

18. A decentralized autonomous method of subdividing a network by optimized clustering; through simulated annealing.

19. A method of enforcing resource allocation levels on links between network nodes that utilize protocols that do not support QOS in their definition or implementation, wherein the method utilizes a network bridge that enables backwards compatibility with existing network protocols that provides relative QOS.

20. A method of broadcasting a communication between nodes of a network that redistribute the communication as needed dependent on the hierarchical relationship of the intended recipients.

21. Technique for preventing circular routes in decentralized dynamic routing networks.

22. A method of decentralized routing that optimally chooses routes based on the current utilization of network resources and the amount of resources requested for a connection.

23. A cryptographic method of dynamically assigning local network addresses.

24. A method of protecting the communication of documents from DOS (denial of service attacks) by limiting the rate at which document communication can occur.

25. A process by which each node of the network is informed of the current resource availability of all links that comprise the network with as little inter-node

communication as possible, wherein the network is informed using full and partial hierarchical flooding techniques.

26. A method of participant, candidate, election enforcement to allow administrative control of elections on networks comprised of non-trusting nodes.